REMARKS/ARGUMENTS

Favorable reconsideration of this application is respectfully requested.

Initially, applicants note an Information Disclosure Statement (IDS) was filed in the present application on May 26, 2006. With the Office Action of July 21, 2006 the filed form PTO-1449 was returned initialing and thereby acknowledging consideration of reference AO. However, applicants note the filed IDS also listed a reference in the "Other References" section as reference AW. The returned form PTO-1449 apparently inadvertently did not initial that reference. Applicants respectfully request a new form PTO-1449 be returned to applicants also acknowledging that "Other Reference" AW.

Claims 5-8, and 11-25 are pending in this application. Claims 1, 2, 3, 9, and 10 are canceled by the present response without prejudice, and new claims 18-25 are added by the present response. Claims 5-8 and 11-17 stand withdrawn from consideration.

Claims 1-2 and 9-10 were rejected under 35 U.S.C. § 103(a) as unpatentable over U.S. patent 6,185,680 to Shimbo et al. (herein "Shimbo") in view of the IBM Technical Disclosure Bulletin NN 8507603 entitled "Matrix Digital Signature for Use With the Data Encryption Algorithm" published on July 1, 1985 (herein "the IBM TDB"). Claims 3 and 4 were rejected under 35 U.S.C. § 103(a) as unpatentable over Shimbo in view of the IBM TDB as applied to claim 1, and further in view of U.S. patent 6,753,313 to Bleichenbacher et al. (herein "Bleichenbacher").

Addressing the above-noted rejections, those rejections are traversed by the present response.

As noted above the previously pending elected claims are canceled by the present response and new claims 18-25 are presented for examination. Those claims are believed to address the outstanding rejections.

The claims are directed to a system which: (i) assigns a device ID in a plurality of device keys corresponding to the device ID, with respect to each of a plurality of content utilizing devices, which decrypt encrypted contents distributed thereto; (ii) encrypts a master key (which is required for decrypting the encrypted contents), so as to enable the device keys (assigned to each content utilizing device) to decrypt the encrypted contents; and (iii) distributes the encrypted master key to the content utilizing device.

In particular the present invention may be directed to technology for inhibiting a content utilizing device targeted for revoke, from decrypting a master key.

According to features in the present invention, (A) each numeral of a device ID indicates a position of a device key in each one dimensional array of a device key matrix. (B) Further, a device ID indicates a path and a plurality of trees that are formed of all possible combinations of device keys in the device key matrix.[1]

(C) A master key is encrypted to enable decryption using path function values calculated from a combination of a device key on a partial path, which is included in the path indicated by a device ID of a device other than the content utilizing device targeted for revoke. The master key is distributed after being encrypted.[2]

(D) The content utilizing device also uses the path function values, which have been calculated based on the device keys, on a partial path that is included in the path indicated by the device ID, to decrypt the master key.[3]

To inhibit the content utilizing device targeted for revoke from decrypting a master key (i.e., to inhibit the device from decrypting the content using the device key on the partial path included in the path indicated by the device ID of the content utilizing device targeted for revoke), (E) a master key is encrypted using path function values calculated from a

[1] See for example the present specification at page 27, line 17 to page 28, line 13.
[2] See for example the present specification at page 28, line 14 to page 33, line 17.
[3] See for example the present specification at page 32, lines 7-25.

combination of device keys on a path that does not include a partial path, which is included in the path indicated by the device ID of the content utilizing device targeted for revoke.[4]

The above-noted features are reflected in new independent claim 18. New independent claims 23 and 25 also recite similar features. The claims as written are believed to clearly distinguish over the applied art.

The outstanding rejection relies on Shimbo to disclose each of the previously recited claim features except that numerals indicating a position of a device key in each one dimensional array of the device key matrix and indicating a path in a plurality of trees that are formed of all possible combinations of device keys in the device key matrix. To cure those recognized deficiencies in Shimbo the outstanding Office Action cites the IBM TDB and particularly at Figure 1 on page 2.

Applicants respectfully submit the above-discussed features recited in new independent claims 18, 23, and 24, clearly distinguish over the applied art.

First, applicants note that the primary reference to Shimbo does not disclose or suggest the features (A)-(E) noted above reflected in the new independent claims. Shimbo also particularly does not disclose or suggest to revoke content decoding at a receiving device. Moreover, the teachings in he IBM TDB do not cure the deficiencies in Shimbo.

Applicants note the matrix described in the IBM TDB is a matrix of cryptographic keys that form an electronic signature. The use of such a matrix completely differs from the use of a device key matrix of the claimed invention. Moreover, the method disclosed in the IBM TDB does not have an object to revoke content decoding at a receiving device, and thereby the IBM TDB does not describe any of the above-noted features of the claimed invention. Thus, the IBM TDB does not cure the deficiencies of Shimbo.

[4] See for example the present specification at page 29, line 6 to page 30, line 20.

In view of the present response applicants respectfully submit the features recited in the claims as written clearly distinguish over Shimbo in view of the IBM TDB.

Moreover, no teachings in Bleichenbacher are believed to cure the above-discussed deficiencies of Shimbo in view of the IBM TDB.

The features recited in new dependent claims 19-22 are believed to even further distinguish over the applied art.

New dependent claim 19 recites each content utilizing device includes a memory to store a device ID assigned to the content utilizing device and a set of path function values each calculated based on one, or a plurality, of device keys of the set assigned to the content utilizing device.[5]

New dependent claim 20 recites each content utilizing device includes a memory to store the device ID and the set of device keys assigned to the content utilizing device.[6]

New dependent claim 22 recites calculating a path function value using a device key on a partial path included in the path indicated by the device ID of a content utilizing device.[7]

New dependent claim 22 indicates each numeral of the device ID, revoke target path, and each of the paths of the boundary set indicates a row in each column of a device key matrix.[8]

In view of the present response, applicants respectfully submit the claims as written are allowable over the applied art.

[5] Support for that claim is, for example, in the present specification at page 39, line 27 to page 40, line 10.

[6] Support for that new claim is, for example, in the present specification at page 39, line 27 to page 40, line 10, and page 32, lines 17-22.

[7] Support for that claim is, for example, in the present specification at page 31, line 16 to page 33, line 10.

[8] Support for that claim is, for example, in the present specification at page 27, line 17 to page 28, line 13; page 29, lines 6-9; and page 30, line 7 to page 31, line 2.

As no other issues are pending in this application, it is respectfully submitted that the present application is now in condition for allowance, and it is hereby respectfully requested that this case be passed to issue.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Surinder Sachar

Eckhard H. Kuesters
Attorney of Record
Registration No. 28,870

Surinder Sachar
Registration No. 34,423

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 03/06)

I:\ATTY\SNS\21's\219406\219406US-AM1.DOC